UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/786,314	02/26/2004	Brig Barnum Elliott	BBNT-P01-265	3449

28120 7590 10/29/2007

ROPES & GRAY LLP
PATENT DOCKETING 39/41
ONE INTERNATIONAL PLACE
BOSTON, MA 02110-2624

EXAMINER	
LAFORGIA, CHRISTIAN A	

ART UNIT	PAPER NUMBER
2131	

MAIL DATE	DELIVERY MODE
10/29/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/786,314	**Applicant(s)** ELLIOTT, BRIG BARNUM	
	Examiner Christian La Forgia	**Art Unit** 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 August 2007*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-37* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-37* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *26 February 2004* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *8/12/07; 10/15/07*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. The amendment of 10 August 2007 has been noted and made of record.

2. Claims 1-37 have been presented for examination.

Response to Arguments

3. Applicant's arguments, see pages 9 and 10, filed 10 August 2007, with respect to the drawings have been fully considered and are persuasive. The objection of Figures 1 and 2 has been withdrawn.

4. Applicant's arguments, see page 10, filed 10 August 2007, with respect to the specification have been fully considered and are persuasive. The objection of the specification has been withdrawn.

5. Applicant's arguments, see page 10, filed 10 August 2007, with respect to the 35 U.S.C. 112, 2nd paragraph rejections have been fully considered and are persuasive. The 35 U.S.C. 112, 2nd paragraph rejections of claims 6-11 have been withdrawn.

6. Applicant's arguments, see page 10, filed 10 August 2007, with respect to the 35 U.S.C. 101 rejections have been fully considered and are persuasive. The 35 U.S.C. 101 rejections of claims 6-11 have been withdrawn.

7. Applicant's arguments, see pages 10 and 11, filed 10 August 2007, with respect to the 35 U.S.C. 101 rejections have been fully considered and are persuasive. The 35 U.S.C. 101 rejections of claims 32 and 33 have been withdrawn.

8. Applicant's arguments regarding the prior art rejections of claims 1-37 have been considered but are moot in view of the new grounds of rejection.

9. See further rejections set forth below.

Claim Rejections - 35 USC § 101

10. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

11. Claims 1-10, 12-21, 23, 26, 30, 34, 35 and 37 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claims 34, 35 and 37 are directed toward the practical application of an abstract idea, and in order to satisfy the 101 requirements, the claim must transform an article or physical object into a different state or thing or otherwise produce a useful, concrete and tangible result. Since the claims merely require "reserving the desired consumption rate" (see similar but not identical claim language), there is no physical transformation and no useful, concrete and tangible result.

Claim Rejections - 35 USC § 103

12. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

13. Claims 1, 2, 6-15, 17-20, 22-24, 26-29, and 31-36 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent Application Publication No. 2005/0036624 to Kent et al., hereinafter Kent, in view of U.S. Patent Application Publication No. 2004/0136321 A1 to Ren et al., hereinafter Ren.

14. As per claims 1 and 31-34, Kent teaches a key agreement protocol in a quantum communication environment wherein a sender transmits binary strings to a receiver and from there the receiver creates a random cryptographic key using the binary strings (Abstract, paragraph 0014).

15. Kent does not teach wherein the receiver requests a certain rate of transfer for the data, the sender determining if it can provide that service to recipient, and, upon determining it can, guaranteeing said transfer rate.

16. Ren teaches issuing a transmission request with a transmission rate, determining whether the specified rate falls within the required transmission rates, and if it does allowing the communication at the specified transmission rate (paragraph 0006).

17. It would have been obvious to one having ordinary skill in the art at the time the invention was made to combine key agreement protocol of Kent with the transmission rate request and determination of Ren, since Ren states at paragraph 0008 that such a modification would maximize system capacity and fulfill users' satisfaction and quality of service requirements. This is further supported by **Quantum Cyrptography on Noisy Channels: Quantum versus Classical Key-Agreement Protocols**, by N. Gisin et al., hereinafter Gisin. Gisin states on page 4201, column 2 and page 4203, column 1, that in a key-agreement protocol similar to that disclosed in Kent, the secret-key rate, or the rate at which Bob and Alice can generate a secret key, should be optimized while minimizing the amount of information available to Eve (representing the eavesdropper).

18. Regarding claim 2, Kent teaches wherein the secret bits are cryptographic key material (paragraph 0003).

19. With regards to claims 6-10, Kent teaches a communication network (Figure 1 [block 16]), which includes using the cryptographic key material to protect traffic flows through an

Ethernet network, an internet, an ATM network, a Synchronous Optical Network (SONET), and Multiprotocol label switching networks, and Official Notice of such is herein taken. U.S. Patent Application No. 2003/0215088 to Bao provides extrinsic evidence, illustrating a similar system, while paragraphs 0083-0116 specifically disclose the various networks that such systems embody.

20. With regards to claim 11, Kent teaches using the cryptographic key material to provide secure communications (paragraph 0030).

21. With regards to claim 12, Kent teaches wherein the first secret bits producing application is based on advantage distillation (paragraph 0028), wherein the Examiner interprets advantage distillation as minimizing the eavesdropper's knowledge of the key.

22. With regards to claim 13, Kent teaches wherein the secret bit producing application is included in a quantum cryptographic system (paragraph 0017).

23. Concerning claims 14 and 15, Kent teaches wherein the quantum cryptographic system employs a laser or a photon source (paragraph 0049).

24. Concerning claim 17, Kent teaches wherein the quantum cryptographic system employs a phase/polarization modulator (paragraphs 0024, 0050).

25. Concerning claims 18 and 19, Kent teaches wherein the quantum cryptographic system employs a free space optical path or an optical fiber path (paragraph 0009).

26. Concerning claim 20, Kent teaches wherein the quantum cryptographic system employs a link comprising photonic band-gap material (Figure 5, paragraphs 0057-0061).

27. Regarding claim 22, Kent teaches using secret bits from the secret bits producing application by a second secret bits consuming application having no requested reserved rate (paragraph 0014).

28. Regarding claim 23, Ren teaches wherein the reservation request includes a priority, a desired rate, and a minimum acceptable bit rate (paragraph 0006, i.e. range of transmission rates includes a minimum acceptable transmission rate).

29. With regards to claim 24, Ren teaches wherein the reserving the first rate comprises:

determining, by the secret bit producing application, whether the desired rate can be satisfied (paragraph 0006, i.e. determining if the transmission rate can be satisfied);

when the desired rate can be satisfied, sending a reply message to the requesting secret bit consuming application indicating a full-success (paragraph 0006, i.e. allowing transmission when the rate can be satisfied);

when the desired rate cannot be satisfied, sending a reply message to the requesting secret bit consuming application indicating a partial-success when an amount of available of the rate is at least enough to satisfy the minimum acceptable rate (paragraph 0006, i.e. allow transmission if rate falls within transmission rate range); and

sending a reply message to the requesting secret bit consuming application indicating a failure to reserve the first rate when neither the desired rate nor the minimum acceptable rate can be satisfied (paragraph 0006, i.e. denying transmission when rate cannot be achieved).

30. Regarding claim 26, Kent teaches determining an estimated bit production rate by the secret bits producing application (paragraph 0017).

31. With regards to claim 27, Kent teaches calculating an available rate of secret bits available for reservations, the calculating comprising calculating a total number of secret bits reserved for a secret bits consuming application; and subtracting the total number of secret bits reserved for a secret bits consuming application from the estimated bit production rate to produce the available rate of secret bits available for reservations (paragraph 0014).

32. Concerning claim 28, Kent discloses the key agreement protocol, which is further detailed in **Unconditionally Secure Key Agreement and the Intrinsic Conditional Information**, by U.M. Maurer, hereinafter Maurer. Maurer teaches on page 500 that the secret-key agreement is always possible when the transfer rate is possible. Therefore, one of ordinary skill in the art could have deleted the at least one lowest priority reservation when the available

rate of secret bits becomes negative, the deleting continuing until the available rate of secret bits becomes non-negative, since a key would not be resolved until the rate was positive.

33. Regarding claim 29, Kent teaches issuing a warning, by the secret bits producing application, when use of secret bits by the first secret bits consuming application from the secret bits producing application exceeds the first rate reserved for the first secret bits consuming application (paragraphs 0011, 0014, i.e. eavesdropper does not know the correct bit and therefore would use too many).

34. As per claim 35, Kent teaches a key agreement protocol that is based on advantage distillation (Abstract, paragraph 0014, paragraph 0028), as supported by page 4201, column 2 of Gisin, which states that the initial phase of the key-agreement protocol is then called advantage distiallation..

35. Kent does not specifying a desired rate by a first process; and reserving the desired rate by the secret bit producer that is based on advantage distillation.

36. Ren teaches issuing a transmission request with a transmission rate, determining whether the specified rate falls within the required transmission rates, and if it does allowing the communication at the specified transmission rate (paragraph 0006).

37. It would have been obvious to one having ordinary skill in the art at the time the invention was made to combine key agreement protocol of Kent with the transmission rate request and determination of Ren, since Ren states at paragraph 0008 that such a modification would maximize system capacity and fulfill users' satisfaction and quality of service

requirements. As noted above, Gisin states on page 4201, column 2 and page 4203, column 1, that in a key-agreement protocol similar to that disclosed in Kent, the secret-key rate, or the rate at which Bob and Alice can generate a secret key, should be optimized while minimizing the amount of information available to Eve (representing the eavesdropper).

38. As per claim 36, Kent teaches a key agreement protocol that is based on advantage distillation (Abstract, paragraph 0014, paragraph 0028), wherein the Examiner interprets advantage distillation as minimizing the eavesdropper's knowledge of the key.

39. Kent does not teach receiving a request from a secure communication process for a reservation of the cryptographic key material at a first rate, the request identifying a minimum acceptable rate; and notifying the secure communication process of a successful reservation when an available generated rate of cryptographic key material is greater than the minimum acceptable rate.

40. Ren teaches issuing a transmission request with a transmission rate, determining whether the specified rate falls within the required transmission rates, and if it does allowing the communication at the specified transmission rate (paragraph 0006).

41. It would have been obvious to one having ordinary skill in the art at the time the invention was made to combine key agreement protocol of Kent with the transmission rate request and determination of Ren, since Ren states at paragraph 0008 that such a modification would maximize system capacity and fulfill users' satisfaction and quality of service requirements. As noted above, Gisin states on page 4201, column 2 and page 4203, column 1, that in a key-agreement protocol similar to that disclosed in Kent, the secret-key rate, or the rate

at which Bob and Alice can generate a secret key, should be optimized while minimizing the amount of information available to Eve (representing the eavesdropper).

42. Claims 3-5 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kent in view of Ren as applied above, and in further view of U.S. Patent Application Publication No. 2001/0038695 to Kim, hereinafter Kim.

43. With regards to claim 3, Kent and Ren do not teach wherein the secret bit producing application is included in a system receiving random or pseudo-random sequences from an external source.

44. Kim teaches wherein the secret bit producing application is included in a system receiving random or pseudo-random sequences from an external source (paragraph 0024).

45. It would have been obvious to one of ordinary skill in the art at the time the invention was made to produce the secret bits using pseudo-random sequences, since Kim states at paragraph 0025 that using a pseudo-random sequence allows the users to exchange data without installing any additional security equipment, thereby making it easier to implement in various types of communication systems.

46. Concerning claim 4, Kim teaches wherein the system is implemented in any communication system (paragraph 0025), which includes systems where the external source is a satellite and Official Notice is taken of such.

47. Concerning claim 5, Kent teaches wherein the random or the pseudo-random sequences are transmitted via radio-frequency signals (paragraphs 0009, 0043).

48. Concerning claim 16, Kent and Ren do not teach a Mach-Zehnder interferometer.

49. Kim teaches a Mach-Zehnder interferometer (paragraphs 0035, 0038).

50. It would have been obvious to one of ordinary skill in the art at the time the invention was made to include an interferometer in the quantum key distribution system, since Kim states at paragraph 0035 that an interferometer can cause time delay or filter certain frequencies in order to determine the coherent interference between the pulses (paragraph 0038).

51. Claims 12, 25, 30, and 37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kent in view of Ren as applied above, and further in view of U.S. Patent No. 6,661,806 to Ericksson et al., hereinafter Ericksson.

52. Regarding claim 21, Kent and Ren do not sending a second reservation request for reserving a second rate from a second secret bit consuming application to the secret bits producing application, wherein the first reservation request and the second reservation request each include a priority of the respective request and the second reservation request has a different priority than the first reservation request.

53. Ericksson teaches sending a second reservation request for reserving a second rate from a second secret bit consuming application to the secret bits producing application, wherein the first reservation request and the second reservation request each include a priority of the respective

request and the second reservation request has a different priority than the first reservation request (column 6, lines 28-47, column 3 lines 48-62).

54. It would have been obvious to one of ordinary skill in the art at the time the invention was made to send a second reservation request for reserving a second rate from a second secret bit consuming application to the secret bits producing application, wherein the first reservation request and the second reservation request each include a priority of the respective request and the second reservation request has a different priority than the first reservation request, since Ericksson states at column 1, lines 17-21 that guaranteeing a level of service ensures the appropriate bandwidth availability, thereby preventing the delay and loss of data.

55. Regarding claim 25, Kent and Ren do not teach canceling a reservation when the secret bits producing application receives a message from the secret bits consuming application indicating that a reservation of the first rate is no longer needed by the secret bits consuming application.

56. Ericksson teaches canceling a reservation when the secret bits producing application receives a message from the secret bits consuming application indicating that a reservation of the first rate is no longer needed by the secret bits consuming application (column 5, lines 10-17).

57. It would have been obvious to one of ordinary skill in the art at the time the invention was made to teaches cancel a reservation when the secret bits producing application receives a message from the secret bits consuming application indicating that a reservation of the first rate is no longer needed by the secret bits consuming application, since it would free up bandwidth that could be reallocated to a different data request, thereby supporting Ericksson statement at

column 1, lines 17-21 of guaranteeing a level of service by ensuring the appropriate bandwidth availability, thereby preventing the delay and loss of data.

58. Regarding claim 30, Kent and Ren do not teach wherein the reserving act reserves the first rate for a limited period of time.

59. Kent teaches wherein the reserving act reserves the first rate for a limited period of time (column 4, lines 57-67).

60. It would have been obvious to one of ordinary skill in the art at the time the invention was made reserve the transmission rate for a predetermined time, since Ericksson states at column 1, lines 17-21 that it would aid in guaranteeing a level of service thereby ensuring the appropriate bandwidth availability, preventing the delay and loss of data.

61. As per claim 37 Kent teaches a key agreement protocol in a quantum communication environment wherein a sender transmits binary strings to a receiver and from there the receiver creates a random cryptographic key using the binary strings (Abstract, paragraph 0014).

62. Kent does not teach specifying a minimum desired consumption râte of secret key material and a priority by a client process; determining, by a secret key material producing process, whether the minimum desired consumption rate of secret key material is available to the client process; when the minimum desired consumption rate of secret key material is not available to the client process, making at least the minimum desired consumption rate of secret key material available by canceling at least one previously made reservation of a rate of the secret key material, each of the at least one previously made reservation having a lower priority

than the specified priority; and reserving at least the minimum desired consumption rate of the secret key material for the client process.

63. Ren discloses specifying a minimum desired consumption rate of data by a client process (paragraph 0006, i.e. range of transmission rates includes a minimum acceptable transmission rate);

determining whether the minimum desired consumption rate of data is available to the client process (paragraph 0006, i.e. determining if it can meet the requested transmission rate); and

reserving at least the minimum desired consumption rate of the data for the client process (paragraph 0006, i.e. allowing communications if the minimum transmission rate is available of the requested transmission rate range).

64. It would have been obvious to one having ordinary skill in the art at the time the invention was made to combine key agreement protocol of Kent with the transmission rate request and determination of Ren, since Ren states at paragraph 0008 that such a modification would maximize system capacity and fulfill users' satisfaction and quality of service requirements. This is further supported by **Quantum Cyrptography on Noisy Channels: Quantum versus Classical Key-Agreement Protocols**, by N. Gisin et al., hereinafter Gisin. Gisin states on page 4201, column 2 and page 4203, column 1, that in a key-agreement protocol similar to that disclosed in Kent, the secret-key rate, or the rate at which Bob and Alice can generate a secret key, should be optimized while minimizing the amount of information available to Eve (representing the eavesdropper).

65. Kent and Ren do not teach a priority and when the minimum desired consumption rate of data is not available to the client process, making at least the minimum desired consumption rate of data available by canceling at least one previously made reservation of a rate of the data, each of the at least one previously made reservation having a lower priority than the specified priority.

66. Ericksson teaches teach a priority and when the minimum desired consumption rate of data is not available to the client process, making at least the minimum desired consumption rate of data available by canceling at least one previously made reservation of a rate of the data, each of the at least one previously made reservation having a lower priority than the specified priority (column 10, lines 12-51, column 9, Table 2, i.e. rejecting reservation request or lowering priority).

67. It would have been obvious to one of ordinary skill in the art at the time the invention was made to include a priority and make at least the minimum desired consumption rate of data available by canceling at least one previously made reservation of a rate of the data, each of the at least one previously made reservation having a lower priority than the specified priority, since Ericksson states at column 1, lines 17-21 that guaranteeing a level of service ensures the appropriate bandwidth availability, thereby preventing the delay and loss of data.

Conclusion

68. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

69. The following patents are cited to further show the state of the art with respect to quantum key-agreement, such as:

United States Patent Application Publication No. 2005/0094818 A1 to Inoue et al., which is cited to show quantum key distribution using the key-agreement protocol.

United States Patent Application Publication No. 2004/0109564 A1 to Cerf et al., which is cited to show a high-rate quantum key distribution scheme.

70. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian La Forgia whose telephone number is (571) 272-3792. The examiner can normally be reached on Monday thru Thursday 7-5.

71. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

72. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Christian LaForgia
Patent Examiner
Art Unit 2131

clf